Data Processing Addendum

This Data Processing Addendum (**"Addendum"**) is effective on the first date that Customer provides to Esri Personal Data (as defined below) subject to the applicable Privacy Law (as defined below) and forms part of the Master Agreement or other written or electronic agreement (**"Agreement"**) by and between the organization signing or accepting below (**"Customer"**) and **Environmental Systems Research Institute, Inc.** (**"Esri"**), and sets forth the terms and conditions relating to the privacy, confidentiality, and security of Personal Data associated with Online Services and subscription and maintenance services to be rendered by Esri to Customer pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified. Terms used in this Addendum that are not defined herein or in the Agreement shall have the meaning set forth in the applicable Privacy Law.

Whereas Customer may provide Esri, a company located in the United States, with access to Personal Data to act as a Processor or Service Provider in connection with Online Services and subscription and maintenance services performed by Esri for or on behalf of Customer pursuant to the Agreement; and

Whereas Customer requires that Esri preserve and maintain the privacy and security of such Personal Data as a Processor according to the terms of this Addendum;

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Esri agree as follows:

SECTION I—DEFINITIONS

A. **"Privacy Laws"** means the European Union (EU) General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the Council of 27 April 2016, the California Consumer Privacy Act of 2018 (CCPA) (as amended by the California Privacy Rights Act [CPRA]), or other privacy laws applicable to Esri.
B. The terms "personal data," "data subject," "processing," "controller," "processor," and "supervisory authority" as used in this Addendum have the meanings given in the GDPR.
C. **"Personal Data"** means personal data, personal information, or personally identifiable information as defined in applicable Privacy Laws about individuals located in the European Union; Switzerland; the United Kingdom; California, USA; or other locations covered by Privacy Laws and may include, but not be limited to, the following: (i) categories of data subjects: prospects, customers, business partners, and vendors; and (ii) types of personal data: name, title, position, email address, and location.
D. **"Data Incident"** means a breach of Esri's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data on systems managed or otherwise controlled by Esri. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial-of-service attacks, and other network attacks on firewalls or networked systems.
E. **"Data Privacy Framework"** means the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

SECTION II—PRIVACY, CONFIDENTIALITY, AND INFORMATION SECURITY

A. Authority to Process Personal Data

   i. Customer and Esri agree that Customer is the Controller and Esri is the Processor or Service Provider of Personal Data, except when Customer is a Processor of Personal Data, then Esri is a subprocessor.
   ii These Addendum terms do not apply where Esri is a Controller of Personal Data (e.g., Personal Data received and Processed by Esri as needed for account setup, authorization, and sign-on in the My Esri self-service portal). Esri's Privacy Statement (available at https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement), together with any related privacy notices or statements, and the Data Transfer Agreement apply where Esri is a Controller.

iii. Esri will Process Personal Data only with Customer's written instructions (a) on behalf of and for the benefit of Customer; (b) for the purposes of Processing Personal Data in connection with the Agreement; and (c) to carry out its obligations pursuant to this Addendum, the Agreement, and applicable Privacy Laws and other law.
iv. Customer will have the exclusive authority to determine the purposes for and means of Processing Personal Data. Esri will not (a) retain, use, or disclose Personal Data outside of the direct business relationship between the parties or for any purpose other than performing under the Agreement, except as otherwise permitted by this Addendum or the Privacy Laws; or (b) combine Customer's Personal Data with any other personal information received or collected from or on behalf of another person, provided that Esri may combine personal information for a business purpose (as defined under CCPA/CPRA).
v. The subject matter and details of the processing are described in Annex I of Attachment 1, and this Addendum (including the Attachment and Annexes) and the Agreement are Customer's complete instructions to Esri for the Processing of Personal Data. Any alternative or additional instructions may only be by written amendment to this Addendum.
vi. To the extent Customer discloses or otherwise makes available deidentified data (as defined in CCPA/CPRA or other Privacy Laws) to Esri or Esri creates deidentified data from Personal Data, Esri shall (a) implement reasonable measures to ensure that such deidentified data is not used to infer information about or otherwise be linked to a particular natural person or household; (b) publicly commit to maintain and use such deidentified data in a deidentified form and not attempt to reidentify the deidentified data; and (c) before sharing deidentified data with any affiliate or third party, including subprocessors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this section. Notwithstanding the prior sentence, Esri may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes are compliant with Privacy Laws.

B. Disclosure of and Access to Personal Data

i. Esri will hold in confidence all Personal Data. Esri will not Sell or Share (as defined in the CCPA/CPRA) Personal Data.
ii. Esri will (a) provide at least the same level of privacy protection for Personal Data received from Customer, as is required by the GDPR, CCPA, and other applicable Privacy Laws, and the Data Privacy Framework principles that may be found on the Data Privacy Framework website; (b) promptly notify Customer if at any time Esri determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Laws and the Data Privacy Framework and (c) take reasonable and appropriate steps to remediate the processing of such Personal Data. If, at any time, Customer notifies Esri that Customer has reasonably determined that Esri is not Processing the Personal Data in compliance with the Privacy Laws, Customer may take reasonable and appropriate steps to stop and remediate any unauthorized Processing of such Personal Data.
iii. If Esri Processes Personal Data provided by Customer that is subject to the GDPR and Esri is established in, or transfers or makes accessible any Personal Data to any subprocessors in a country that does not ensure adequate data privacy safeguards are in place within the meaning of GDPR, then Esri will enter into the standard contractual clauses with Customer as set forth in Attachment 1 of this Addendum ("SCCs") or ensure that adequate data privacy safeguards are in place, such as binding corporate rules or the Data Privacy Framework certification. If applicable, each party's signature to this Addendum shall be considered a signature to the SCCs. If a subprocessor is a Data Importer (as that term is used in such SCCs), Esri shall either (a) enter into contractual obligations with subprocessor, where such obligations contain adequate privacy safeguards in accordance with GDPR, or (b) enter into the SCCs with Customer on behalf of such data importer. In the event the transfer is covered by more than one transfer mechanism, the transfer of personal data will be subject to a single transfer mechanism, as applicable, and in accordance with the following order of precedence: (a) the Data Privacy Framework; (b) the SCCs; and if neither of the preceding is applicable, then (c) other alternative data transfer mechanisms permitted under applicable Privacy Laws will apply.
iv. Esri will not share, transfer, disclose, or otherwise provide access to any Personal Data to any third party, or contract any of Esri's rights or obligations concerning Personal Data to a third party, unless Customer has authorized Esri to do so in writing, except as required by law. Where Esri, with the consent of Customer, provides to a third party access to Personal Data or contracts such rights or obligations to a third party, Esri

will, with each third party, (a) enter into a written agreement that imposes obligations on the third party that are consistent with the GDPR, CCPA, and the other Privacy Laws; (b) transfer the Personal Data to the third party only for the limited and specified purposes as instructed by Customer; (c) require the third party to notify Esri if the third party determines that it can no longer meet its obligation to provide the same level of protection as is required by the applicable Privacy Laws; and (d) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing. Customer hereby provides its consent for Esri to use subprocessors as necessary to provide the services including, but not limited to, Microsoft Corporation; Amazon Web Services, Inc.; Salesforce, Inc.; and Akamai Technologies (including their affiliates) and Esri's technical support vendors. To the extent that Esri makes any changes with regard to the use of its subprocessors, it shall inform Customer and provide Customer with the right to object to such change. To the extent Customer has a reasonable objection to such change in subprocessors, the parties shall cooperate to address the objection in a reasonable manner.

v. Esri will promptly inform Customer in writing of any requests with respect to Personal Data received from Customer's customers, consumers, employees, or other associates. Customer will be responsible for taking action on and responding to any such request, but Esri will reasonably cooperate with Customer to address any such request or a request by an individual about whom Esri holds Personal Data for access, rectification, objection, portability, restriction, erasure, or export of that individual's Personal Data. For clarity, Customer is a Controller of Named User Credentials, as defined in the Master Agreement. Customer is solely responsible for taking action on and responding to any data subject requests associated with Named User Credentials.

vi. Taking into account the state of the art; the costs of implementation; and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity of the rights and freedoms of natural persons, Esri will implement appropriate technical and organizational measures to protect the Personal Data from loss; misuse; and unauthorized access, disclosure, alteration, and destruction. Such measures are set forth in Annex II of Attachment 1. To this effect, Esri will limit internal access to Personal Data so that it is only accessible on a need-to-know basis to fulfill Esri's performance of services for or on behalf of Customer, by personnel who have agreed to comply with privacy and security obligations that are substantially similar to those required by this Addendum.

vii. Subject to applicable law, Esri will notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer may, if it so chooses, seek a protective order, and Esri will reasonably cooperate with Customer in such action, provided Customer reimburses Esri for all costs, fees, and legal expenses associated with the action. Esri will have the right to approve or reject any settlements that affect Esri.

viii. If Esri becomes aware of a Data Incident, Esri will (a) notify Customer of the Data Incident promptly and without undue delay after becoming aware of the Data Incident; and (b) promptly take reasonable steps to minimize harm and secure Personal Data. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Esri recommends Customer take to address the Data Incident. Esri will not assess the contents of Personal Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any notification obligations to third parties related to any Data Incident(s). Esri's notification of or response to a Data Incident under this section will not be construed as an acknowledgement by Esri of any fault or liability with respect to the Data Incident.

C. Esri currently has the third-party certifications and review processes in place as described at https://trust.arcgis.com. Esri participates in and has certified its compliance with Data Privacy Framework.

D. Esri will comply with applicable data protection and privacy laws, including, but not limited to, the GDPR and CCPA, to the extent such laws apply to Esri in its role as Processor or Service Provider.

E. Customer certifies that it has

i. Obtained the written consent, affirmative opt-in, or other written authorization ("**Consent**") from applicable individuals or has another legitimate, legal basis for delivering or making accessible Personal Data to Esri (as well at its subsidiaries, affiliates, and subprocessors), and such Consent or other legitimate basis allows Esri (and its subsidiaries, affiliates, and subprocessors) to Process the Personal Data pursuant to the terms of the Agreement and this Addendum; and

ii. Ensured that the delivery and disclosure to Esri of Personal Data is in compliance with the GDPR, CCPA, and other Privacy Laws that are applicable to Customer.

F. Esri will assist Customer in ensuring that its secure Processing obligations, as Controller, under the GDPR are met, which may include assisting Customer in a consultation with a supervisory authority where a data protection impact assessment indicates that the intended Processing would result in a high level of risk. Upon request, Esri shall make available to Customer the information necessary to demonstrate compliance with the GDPR and will allow for and contribute to audits, including inspections, to confirm Esri's compliance with this Addendum by Controller or another auditor mandated by Controller. At Customer's request to verify compliance, Esri will provide to Customer a summary of its most recent independent third-party audit results or similar self-assessment. The summary will be provided no more than once annually, and disclosure of the summary will be subject to a written nondisclosure agreement between the parties. An on-site audit may be conducted by Customer or an independent third-party auditor as agreed by the parties when (i) such an audit is required by Privacy Law or Customer's competent supervisory authority; and (ii) Customer has received a notice from Esri of a Data Incident affecting Customer's Personal Data. The scope and scheduling of such audit will be mutually agreed upon by the parties in advance. Any on-site audits will be limited to Customer Content processing and storage facilities operated by Esri. Customer acknowledges that Esri operates a multitenant cloud environment. Accordingly, Esri shall have the right to reasonably adapt the scope of any on-site audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Esri customers' information. All expenses resulting from this Subsection F will be incurred by Customer, unless Esri is found materially noncompliant. Customer must promptly notify Esri of any discovered noncompliance.

G. Upon fulfillment of the purpose for which Customer provided Personal Data under this Addendum, Esri shall either return all Personal Data Processed on behalf of Customer or delete or destroy the Personal Data, including any existing copies, at Customer's expense, if any, unless Esri has a legal obligation to maintain such Personal Data.

H. Trial, Evaluation, and Beta Program offerings may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use trial, evaluation, and beta program offerings to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this Addendum do not apply to trial, evaluation, and beta program offerings: Processing of Personal Data, GDPR, Data Security, and Health Insurance Portability and Accountability Act (HIPAA) Business Associate.

CUSTOMER CERTIFIES THAT IT AND ITS EMPLOYEES UNDERSTAND THESE RESTRICTIONS AND WILL COMPLY WITH THEM.

IN WITNESS WHEREOF, the parties acknowledge their agreement to the foregoing by due execution of this Addendum by their respective authorized representatives. The Addendum cannot be modified or amended by either party except with a separate written document signed by both parties.

_____	ENVIRONMENTAL SYSTEMS RESEARCH INSTITUTE, INC.
(Customer)	(Esri)
By: _____	By: _____
Authorized Signature	Authorized Signature
Printed Name: _____	Printed Name: Tamisa Greening
Title: _____	Title: Director, Contracts and Legal
Date: _____	
Customer Number: _____	

ATTACHMENT 1
STANDARD CONTRACTUAL CLAUSES IMPLEMENTATION

1. The Parties agree that, with respect to the implementation of the EU Standard Contractual Clauses (Commission Decision 2021/914) (“SCCs”) under the Addendum, one or more of the following Modules of the SCCs will apply and are referenced herein: (i) Controller to Processor ("Module Two" or "C2P"); (ii) Processor to Processor ("Module Three" or "P2P").

2. To the extent one or more of the foregoing SCCs apply, the Parties agree to the following:

   a) Clause 7 (Docking Clause) shall not apply;
   b) The Option 2 (General Written Authorisation) provision of Clause 9(a) (Use of subprocessors) shall apply, and the specified time period shall be thirty (30) days;
   c) The Clause 11(a) (Redress) option shall not apply;
   d) Governing law under Clause 17 (Governing law) shall be law of the Republic of Ireland; and
   e) Clause 18 (Choice of forum and jurisdiction) shall mean the courts of the Republic of Ireland.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name:** As identified in the Agreement and this Addendum

   Address: Per Esri's customer service records

   Contact person's name, position and contact details: Per Esri's customer service records

   Activities relevant to the data transferred under these Clauses: Online Services and subscription and maintenance services to be rendered by Esri to Customer

   Signature and date: Each party's signature of the Addendum shall be considered a signature to these Clauses.

   Role (controller/processor): Controller

Data importer(s):

1. **Name:** Environmental Systems Research Institute, Inc. ("Esri")

   Address: 380 New York Street, Redlands, CA 92373, USA

   Contact person's name, position, and contact details: Chief Information Security Officer, privacy@esri.com

   Activities relevant to the data transferred under these Clauses: Online Services and subscription and maintenance services to be rendered by Esri to Customer

   Signature and date: Each party's signature of the Addendum shall be considered a signature to these Clauses.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data about individuals is provided to Esri via the Online Services and subscription and maintenance services by (or at the direction of) Customer or by Customer end users, who may include Customer's customers, employees, suppliers, and End Users.

Categories of personal data transferred

Data related to individuals is provided to Esri via the Online Services and subscription and maintenance services, by (or at the direction of) Customer or by Customer end users.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), recordkeeping of access to the data, restrictions for onward transfers, or additional security measures

Considering that only Customer (not Esri) has full knowledge and control in relation to what data is provided to Esri via the Online Services and subscription and maintenance services, Esri treats all Customer Content to the standards of sensitive data by providing the technical and organizational measures described in Annex II. Customer is responsible for verifying that such measures are appropriate for the specific categories of data provided to Esri via the Online Services and subscription and maintenance services.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

The frequency of the transfer depends on the frequency at which Customer provides Personal Data to Esri via the Online Services and subscription and maintenance services. It is expected that transfers may be on a one-off and/or continuous basis.

Nature of the processing

Spatial analytics is accomplished through the following operations, dependent on Customer's choice of settings and actions performed: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other method of making available, alignment or combination, restriction, or erasure or destruction.

Purpose(s) of the data transfer and further processing

Esri will process Personal Data for the purposes of providing the Online Services and subscription and maintenance services to Customer in accordance with the Agreement.

The period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained depends on the duration of processing as determined by Customer and Customer's additional instructions.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Cloud services and technical support services involve processing of the same nature and duration as described above.

C. COMPETENT SUPERVISORY AUTHORITY

As applicable, competent supervisory authority will be in accordance with Clause 13.

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Esri will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to ArcGIS Online Services and subscription and maintenance services, as described in the Security and Privacy Documentation applicable to the specific ArcGIS Online Services and subscription and maintenance services purchased by the data exporter, as updated from time to time, and accessible via https://trust.arcgis.com/en/security/security-overview.htm or otherwise made reasonably available by Esri.

A. Technical Measures for ArcGIS Online Services. Esri implemented the following technical measures for the above-referenced ArcGIS Online Services:

i. The state-of-the-art encryption algorithm and its parameterization (e.g., key length; operating mode, if applicable) are used for Customer data at rest.
ii. The strength of the encryption takes into account the time period during which the confidentiality of the encrypted personal data must be preserved.
iii. The encryption algorithm is implemented by properly maintained software, the conformity of which to the specification of the algorithm chosen has been verified by certification.
iv. The keys are reliably managed (generated, administered, stored, linked to the identity of an intended recipient, and revoked).
v. ArcGIS Online allows Customer (data exporter) to pseudonymize the fields (e.g., user credentials) in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information exclusively held and controlled by Customer (data exporter), of which Customer (data exporter) retains sole control of the algorithm or repository that enables reidentification using additional information.
vi. ArcGIS Online supports best practices for transport encryption protocols.
vii. A trustworthy public key certification authority and infrastructure are used.
viii. Specific protective and state-of-the-art measures are used against active and passive attacks.
ix. The existence of backdoors (in hardware or software) has been ruled out.
x. ArcGIS Online can be used in combination with ArcGIS Enterprise in a configuration that allows Customer (data exporter) to store and manage Personal Data under Customer's (data exporter's) control without transferring it to a third country, whereas a data exporter processes Personal Data in such a manner that it is split into two or more parts, and the part that is being transferred to the third country can no longer be interpreted or attributed to a specific data subject without the use of additional information under Customer's (data exporter's) control.

Additional information on technical measures can be found at https://trust.arcgis.com/en/documents/.

B. Organizational and Contractual Measures

i. Esri's efforts around privacy are described at https://www.esri.com/en-us/privacy/overview.
ii. Esri commits to treating Personal Data per its Privacy Statement (available at https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement) and the Esri Products & Services Privacy Statement Supplement (available at https://www.esri.com/en-us/privacy/privacy-statements/privacy-supplement).
iii. Esri provides a presigned Data Processing Addendum that contains Standard Contractual Clauses, available at https://www.esri.com/en-us/privacy/privacy-gdpr.
iv. Esri maintains and enforces an internal personal information protection policy that requires employees to protect Personal Data that they access.
v. Esri maintains a corporate security policy that addresses access controls and corporate security measures.

C. Adoption of Further Requirements and Right to Early Termination. If supervisory authorities adopt further requirements and measures with regard to the transfer of Personal Data to the US, Esri will amend this Addendum to fulfill the additional requirements. If Esri cannot meet the additional requirements, Customer shall have the right to terminate the Agreement for convenience (without termination fee or penalty) by giving written notice thereof to Esri.